

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Eui-hyeon HWANG et al.

Application No.:

Group Art Unit:

Filed: January 21, 2004

Examiner:

For: USER AUTHENTICATION METHOD AND APPARATUS

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

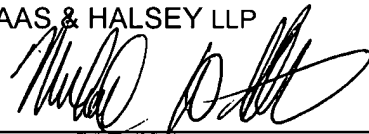
Republic of Korea Patent Application No(s). 2003-4103

Filed: January 21, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP



Date: January 21, 2004

By: \_\_\_\_\_

Michael D. Stein  
Registration No. 37,240

1201 New York Ave, N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원번호 : 10-2003-0004103  
Application Number

출원년월일 : 2003년 01월 21일  
Date of Application JAN 21, 2003

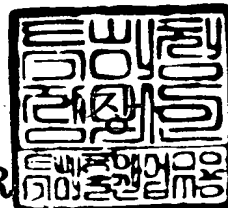
출원인 : 삼성전자주식회사  
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 년 02 월 07 일

특 허 청

COMMISSIONER



## 【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0009
【제출일자】	2003.01.21
【국제특허분류】	G06F
【발명의 명칭】	사용자 인증 방법 및 장치
【발명의 영문명칭】	Method and apparatus for user authentication
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2003-003435-0
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2003-003436-7
【발명자】	
【성명의 국문표기】	황의현
【성명의 영문표기】	HWANG, Eui Hyeon
【주민등록번호】	720920-1067323
【우편번호】	420-751
【주소】	경기도 부천시 원미구 상1동 반달마을아파트 1804동 1705호
【국적】	KR
【발명자】	
【성명의 국문표기】	이종하
【성명의 영문표기】	LEE, Jong Ha
【주민등록번호】	740117-1691611
【우편번호】	445-974

**【주소】** 경기도 화성군 태안읍 병점리 우남드림밸리 1차아파트 104동 301호  
**【국적】** KR  
**【심사청구】** 청구  
**【취지】** 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인  
 이영필 (인) 대리인  
 이해영 (인)  
**【수수료】**  
**【기본출원료】** 20 면 29,000 원  
**【가산출원료】** 10 면 10,000 원  
**【우선권주장료】** 0 건 0 원  
**【심사청구료】** 21 항 781,000 원  
**【합계】** 820,000 원  
**【첨부서류】** 1. 요약서·명세서(도면)\_1통

**【요약서】****【요약】**

사용자 인증 방법이 개시된다. 외부로부터 입력된 하나 이상의 숫자 또는 문자에 의한 비밀번호와, 지문, 홍채, 얼굴 등의 사용자의 생체 인식 정보에 의하여 사용자를 인증하는 본 발명에 의한 사용자 인증 방법은, (a) 비밀번호가 입력되었는가를 판단하는 단계; (b) 비밀번호가 입력된 경우에, 비밀번호가 등록된 비밀번호와 일치하면 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정하고, 비밀번호가 등록된 비밀번호와 일치하지 않으면 FAR을 낮춘 제2 문턱값으로 설정하는 단계; 및 (c) 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 상기 (a) 단계로 진행하는 단계를 포함하는 것을 특징으로 한다. 따라서, 비밀번호와 생체 인식기가 유기적으로 결합하여 비밀번호의 입력 결과가 생체 인식기 성능에 영향을 주거나, 생체 인식 결과가 피드백되어 다음의 인증과정에 영향을 주도록 하여 FAR(False Acceptance Rate)와 FRR(False Rejection Rate)를 함께 향상시키는 효과가 있다.

**【대표도】**

도 1

**【명세서】****【발명의 명칭】**

사용자 인증 방법 및 장치{Method and apparatus for user authentication}

**【도면의 간단한 설명】**

도 1은 본 발명에 의한 사용자 인증 방법의 바람직한 일 실시예를 설명하기 위한 플로우차트이다.

도 2는 도 1에 도시된 실시예에, 비밀번호 입력 히스토리를 저장 및 분석하여 침입 여부 결정하는 단계들이 추가된 실시예를 설명하기 위한 플로우차트이다.

도 3은 도 1에 도시된 실시예에, 비밀번호 입력 히스토리를 저장 및 분석하여 비밀번호 입력 히스토리에 따라 생체 인식기의 문턱값을 변경하는 단계들이 추가된 실시예를 설명하기 위한 플로우차트이다.

도 4는 도 1에 도시된 실시예에, 인증키를 갱신하는 단계들이 추가된 실시예를 설명하기 위한 플로우차트이다.

도 5는 도 1 내지 도 4에 도시된 실시예들이 모두 결합된 실시예를 설명하기 위한 플로우차트이다.

도 6은 본 발명에 의한 사용자 인증 장치의 바람직한 일 실시예를 설명하기 위한 블록도이다.

**【발명의 상세한 설명】****【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <7> 본 발명은 사용자 인증에 관한 것으로서, 특히 비밀번호와 생체 인식의 결합에 의한 사용자 인증에 관한 것이다.
- <8> 비밀번호와 생체 인식기를 결합한 형태의 종래 인증기 기술로는 다음과 같은 것들이 있다.
- <9> 국내특허출원 제2000-19152호 "휴대용 보안 인증 장치 및 시스템 그리고 그의 동작 방법"은 지문, 음성등의 생체 인증과 패스워드 입력의 순차적 결합에 의한 인증 방법을 개시하고 있다.
- <10> 국내특허출원 제2000-3099호 "지문 인증과 비밀번호 인증 겸용 방식을 채용한 도어 록/언록 시스템 및 그 제어 방법"은 지문등록이 불가능한 사용자의 사용을 가능하게 함과 동시에 지문등록이 이루어지지 않은 방문객도 비밀번호를 사용하여 사용자 인증을 받을 수 있는 지문인증과 비밀번호 인증 겸용방식을 채용한 도어 록/언록 시스템 및 그 제어방법을 개시하고 있다.
- <11> 국내특허출원 제2000-60312호 "지문 인식 및 얼굴 인식을 이용한 출입 통제 시스템 및 그 방법"은 지문 인식과 얼굴 인식을 통한 사용자 인증, 비밀번호인증과 지문 인식과 얼굴 인식을 통한 사용자 인증, 및 인증되지 않은 출입자의 지문 및 얼굴을 저장하여 보안성을 향상시키는 출입 통제 시스템 및 그 방법을 개시하고 있다.

- <12> 그 밖에 국내특허출원 제2001-15559호 "지문인식을 이용한 도어개폐시스템", 국내 특허출원 제1999-26726호 "음성인식을 통한 휴대폰의 비밀번호 인식방법" 등 다수가 있다.
- <13> 전술한 종래의 사용자 인증 방법들은 비밀번호와 생체인식, 또는 보안열쇠와 생체인식을 단순히 결합하여 복수의 인증 절차를 거치게 하는 형태이다.
- <14> 얼굴, 지문, 홍채 등의 인증키에 의한 생체인식기는 사용 환경, 사용자의 사용습관, 시간에 따른 인증키의 변화 등으로 인하여 인증키 자체가 생체 인식기에 다르게 입력되어 인식 성능이 저하된다.
- <15> 열쇠, 비밀번호, IC카드, RF카드 등의 경우에, 키가 입력되면 그 결과가 "0" 또는 "1" 개념으로 2치화 되지만, 생체 인식기의 경우는 입력되는 인증기 성능 및 인증키 자체의 변화에 의해 등록된 데이터와의 정합정도에 따라 인증 결과가 "0~1" 사이의 값으로 나타난다. 따라서 거부(0)/인증(1)을 구분하기 위하여는 적절한 문턱치 설정이 필요하다. 만일 인증 문턱치를 높인다면, 등록되지 않은 사람이 인증될 확률이 낮아지지만, 상대적으로 등록된 사람이 인증되지 않을 확률이 높아진다. 따라서 문턱치 설정에 따라 등록된 사람이 인증되지 못하거나(FR: False Rejection), 등록되지 않은 사람이 인증되는 오류(FA: False Acceptance)가 발생하게 된다.

**【발명이 이루고자 하는 기술적 과제】**

- <16> 따라서 본 발명이 이루고자 하는 기술적 과제는, 비밀번호와 생체 인식을 조합하여 등록된 사람이 인증되지 못하는 확률(FAR : False Acceptance Rate)과 등록되지 않은 사



람이 인증되는 확률(FRR : False Rejection Rate)을 함께 낮출 수 있는 사용자 인증 방법을 제공하는 데 있다.

<17> 또한 본 발명이 이루고자 하는 다른 기술적 과제는, 상기 사용자 인증 방법을 수행하는 사용자 인증 장치를 제공하는데 있다.

#### 【발명의 구성 및 작용】

<18> 상기한 기술적 과제를 이루기 위해, 외부로부터 입력된 하나 이상의 숫자 또는 문자에 의한 비밀번호와, 지문, 홍채, 얼굴 등의 사용자의 생체 인식 정보에 의하여 사용자를 인증하는 본 발명에 의한 사용자 인증 방법은, (a) 비밀번호가 입력되었는가를 판단하는 단계; (b) 비밀번호가 입력된 경우에, 상기 비밀번호가 등록된 비밀번호와 일치하면 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정하고, 상기 비밀번호가 등록된 비밀번호와 일치하지 않으면 FAR을 낮춘 제2 문턱값으로 설정하는 단계; 및 (c) 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 상기 (a) 단계로 진행하는 단계를 포함하는 것이 바람직하다.

<19> 상기한 다른 기술적 과제를 이루기 위해, 외부로부터 입력된 하나 이상의 숫자 또는 문자에 의한 비밀번호와, 지문, 홍채, 얼굴 등의 사용자의 생체 인식 정보에 의하여 사용자를 인증하는 본 발명에 의한 사용자 인증 장치는, 외부로부터 비밀번호가 입력되었는가를 판단하는 비밀번호 입력부; 비밀번호가 입력된 경우에, 상기 비밀번호가 등록된 비밀번호와 일치하면 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정하고, 상기 비밀번호가 등록된 비밀번호와 일치하지 않으면 FAR을 낮춘 제2 문턱값

으로 설정하는 문턱값 설정부; 및 상기 사용자의 생체 인식 정보를 입력하여 사용자가 인증되었는가를 결정하는 생체 인식기를 포함하는 것이 바람직하다.

<20> 이하, 본 발명에 의한 사용자 인증 방법 및 장치의 구성과 동작을 첨부한 도면들을 참조하여 다음과 같이 설명한다.

<21> 본 발명은 하나 이상의 숫자 또는 문자에 의한 비밀번호(입력수단)와, 지문, 홍채, 얼굴 등의 생체 인식(입력수단)에 의하여 사용자를 인증하는 방법이다. 비밀번호는 단말기에 마련된 숫자 버튼, 터치 패널 등의 키 입력 장치 및 이와 동등한 기능의 입력 수단에 의하여 입력될 수 있다.

<22> 본 발명에 있어서 사용되는 생체 인식의 인증 지표는 FAR(False Acceptance Rate)와 FRR(False Rejection Rate)의 두가지가 있다. FAR은 등록되지 않은 사람 즉 침입자가 인증될 확률이고, FRR은 등록된 사람 즉 주인이 인증되지 못 할 확률로서, 양자 모두 인증 실패에 관한 지표이다. FAR을 낮추면 침입자가 인증될 확률이 낮아지므로, 보안성이 높아진다. 반대로 FRR을 낮추면 주인이 인증되지 못 할 확률이 낮아지므로, 주인의 편의성이 높아진다. 생체 인식기의 성능은 문턱치의 조정에 의하여 변동되는데, 이 때 FAR과 FRR은 상호 트레이드 오프(trade off)한다.

<23> 본 발명에 의한 사용자 인증 방법은 개인 컴퓨터로의 진입 통제 수단, 개인 휴대 단말의 사용 통제 수단, 인터넷 서비스에의 접속 통제 수단, 보안 시설에의 출입 통제 수단에 적용되어 사용될 수 있다.

- <24> 도 1은 본 발명에 의한 사용자 인증 방법의 바람직한 일 실시예를 설명하기 위한 플로우차트로서, 입력된 비밀 번호의 일치여부에 따라 생체 인식기의 문턱값을 가변하여 사용자를 인증하는 단계들(S100 ~ S108 단계)로 이루어진다.
- <25> 생체 인식기는 등록된 생체 인식 정보와 입력된 생체 인식 정도와의 정합 정도에 따라 보안 수준이 조절된다. 즉 정합 정도가 소정 문턱값 이상이면 사용자가 인증되고, 그렇지 않으면 거부된다. 인증을 위한 문턱값을 높게 설정하여 침입자를 완벽하게 차단하려 하면, 본인마저 통과하지 못할 수도 있다. 반대로 본인을 쉽게 통과하게 하면, 침입자가 통과할 가능성도 커진다. 즉, 본인의 편의성을 위하여 FRR을 낮출 경우 FAR이 높아지고, 침입에 대한 보안성을 위하여 FAR을 낮출 경우 FRR이 높아지는 결과를 낳는다.
- <26> 본 발명에 있어서는 비밀번호의 일치 여부에 따라 이중 문턱값을 적용한다. 비밀번호가 올바르게 입력된 경우에는 FRR이 낮아지도록 인증 문턱치를 낮추어서, 본인의 편의성을 높인다. 반대로 비밀번호가 올바르게 입력되지 않은 경우에는, 본인의 편의성 보다는 침입에 대한 보안성을 강화하도록 한다. 이를 위하여 구비되는 단계들을 다음과 같이 설명한다.
- <27> 먼저 S100 단계에서는, 비밀번호가 입력되었는가를 계속적으로 판단한다. S100 단계를 위하여는 인증기에 표시부를 마련하여, 비밀번호를 입력할 것을 표시할 수 있다.
- <28> S102 단계에서는, 입력된 비밀번호가 등록된 비밀번호와 일치하는가를 판단한다.
- <29> S104 단계에서는, 입력된 비밀번호가 등록된 비밀번호와 일치하는 경우에는, 생체 인식기에서 사용되는 문턱값을 FRR을 소정 레벨로 낮춘 제1 문턱값으로 설정한다.

- <30> S106 단계에서는, 입력된 비밀번호가 등록된 비밀번호와 일치하지 않는 경우에는, 생체 인식기에서 사용되는 문턱값을 FAR을 소정 레벨로 낮춘 제2 문턱값으로 설정한다.
- <31> S108 단계에서는, 상기 제1 및 제2 문턱값이 설정된 생체 인식기에 의해 사용자가 인증되었는가를 판단하여, 사용자가 인증되지 않은 경우에는 S100 단계로 진행한다.
- <32> 표 1은 도 1에 도시된 이중 문턱값을 적용하는 사용자 인증 방법의 구체적인 일 실시예를 설명하기 위하여 문턱값 변화에 따른 FAR과 FRR의 변화를 보인 것이다.

<33> 【표 1】

FAR (%)	0.00	0.01	0.10	0.20	0.50	1.00	2.00
FRR (%)	41.48	26.25	17.41	15.28	10.42	8.24	6.43

- <34> 표 1을 참조하면, FAR이 낮으면 FRR이 높고, FRR이 낮으면 FAR이 높아진다는 것을 알 수 있다. 사용자를 인증함에 있어서는 FAR과 FRR이 모두 낮은 것이 가장 바람직하다.
- <35> 예컨대 개인 휴대용 단말기(PDA, personal digital assistant)에서 비밀번호를 입력할 수 있는 키 조작부의 버튼 수가 10개인 경우, 비밀번호가 한 자리수라고 가정하고, 본 발명에 의한 사용자 인증 방법을 다음과 같이 설명한다.
- <36> 먼저 (FAR, FRR)의 이중 문턱값으로서, 비밀번호를 올바르게 입력할 경우에는 (1.00%, 8.24%)를 이용하고, 틀리게 입력할 경우에는 (0.10%, 17.41%)를 이용하도록 설정한다. 버튼 수가 10개이므로, 침입자가 한 번의 시도로 비밀번호를 올바르게 입력할 확률은 10 % (=0.1) 이고, 비밀번호를 틀리게 입력할 확률은 90 % (=0.9) 이다. 또한 본인이 한 번의 시도로 비밀번호를 올바르게 입력할 확률을 100% 이고, 틀리게 입력할 확률은 0%라 가정한다. 따라서, 비밀번호와 문턱치 조합에 의하여 얻어지는 본인이 통과하지 못할 FRR과 침입자가 통과할 FAR은 다음 수학적 식 1과 같다.

<37> 【수학식 1】  $FRR = 1.0 \times 8.24 + 0.0 \times 17.41 = 8.24 \%$

<38>  $FAR = 0.1 \times 1.00 + 0.9 \times 0.10 = 0.19 \%$

<39> 결국 본 발명에 의한 이중 문턱값을 적용하는 사용자 인증 방법에 의하여 얻어지는 (FAR, FRR) 성능은 (0.19%, 8.24%) 이다. 이러한 결과는, 하나의 문턱치만을 이용하여 사용자 인증을 수행했을 경우보다, FAR은 0.19% 로 낮아져서 침입자가 통과할 가능성이 낮아진다. 이 때, 문턱값만에 의한다면 FAR 0.19%에 대응하는 FRR은 약 15.28%이겠지만, 본 발명에 의한 FRR은 8.24%이므로, 본인이 거부될 가능성도 낮아진다.

<40> 만일 두 자리의 비밀번호를 사용한다면, 침입자가 한 번의 시도로 비밀번호를 올바르게 입력할 확률은 1 % (=0.01) 이고, 비밀번호를 틀리게 입력할 확률은 99 % (=0.99) 이다. 이때, 비밀번호와 문턱치 조합에 의하여 얻어지는 본인이 통과하지 못 할 FRR과 침입자가 통과할 FAR은 다음 수학식 2와 같이 FAR이 더욱 향상된 결과를 얻게 되고 이에 따라 인식기의 성능이 향상된다.

<41> 【수학식 2】  $FRR = 1.0 \times 8.24 + 0.0 \times 17.41 = 8.24 \%$

<42>  $FAR = 0.01 \times 1.00 + 0.99 \times 0.10 = 0.109 \%$

<43> 도 2는 도 1에 도시된 실시예에, 비밀번호 입력 히스토리를 저장 및 분석하여 침입 여부 결정하는 단계들이 추가된 실시예의 플로우차트이다. 침입자인 경우에 비밀번호를 모르고 인증을 시도할 것이다. 반면에 등록된 본인이라도 실수로 비밀번호를 잘못 입력할 경우가 있을 것이다. 예컨대 생체 인식에 의한 사용자 인증이 수회 반복되는 과정에서 잘못된 비밀 번호가 n회 이상 입력되었다면, 침입으로 판단할 수 있다. 만일 침입으로 판단되면, 계속되는 인증 시도를 방지하기 위하여, 입력된 침입자의 생체 인식 정보

를 저장하고 이를 기준으로 침입자를 거부하거나 인증 문턱치를 최대치로 올려서 침입자의 인증을 차단할 수 있다. 이를 위하여 구비되는 단계들을 다음과 같이 설명한다.

- <44>        먼저 S200 단계에서는, 비밀번호가 입력되었는가를 계속적으로 판단한다.
- <45>        S202 단계에서는, 입력된 비밀번호가 등록된 비밀번호와 일치하는가를 판단한다.
- <46>        S204 단계에서는, 입력된 비밀번호가 등록된 비밀번호와 일치하는 경우에는, 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정한다.
- <47>        S206 단계에서는, 입력된 비밀번호가 등록된 비밀번호와 일치하지 않는 경우에는, 생체 인식기에서 사용되는 문턱값을 FAR을 낮춘 제2 문턱값으로 설정한다.
- <48>        S208 단계에서는, 비밀번호 입력 히스토리를 저장한다. 예컨대 잘못된 비밀번호가 입력되는 경우에 +1씩 카운트하게 할 수 있다.
- <49>        S210 단계에서는, 제1 또는 제2 문턱값이 설정된 생체 인식기에 의해 사용자가 인증되었는가를 판단한다.
- <50>        S212 단계에서는, 사용자가 인증되지 않은 경우에 비밀번호 입력 히스토리를 이용하여 침입여부를 판단하여, 침입이 아니라고 판단되면 S200 단계로 진행한다. 그러나 만일 침입이라고 판단되면, 사용자 인증 방법을 종료하거나, 생체 인식의 문턱치를 최대치로 설정하고 S200 단계로 진행할 수 있다.
- <51>        또한 침입이라고 판단되는 경우에, 침입자 생체 인식 정보를 저장하고 이를 생체 인식기에 의한 사용자 인증에 활용할 수도 있다. 이를 위하여, S212 단계의 판단 결과 침입이라고 판단되면, 입력된 침입자의 생체 인식 정보를 저장하는 단계(S214 단계)를

더 포함할 수 있다. 이 때, S210 단계는 생체 인식기 입력값과 S214 단계에서 저장된 침입자의 생체 인식 정보를 비교하여 인증하는 단계를 더 포함할 수 있다.

<52> 도 3은 도 1에 도시된 실시예에, 비밀번호 입력 히스토리를 저장 및 분석하여 비밀번호 입력 히스토리에 따라 생체 인식기의 문턱값을 변경하는 단계들이 추가된 실시예를 설명하기 위한 플로우차트이다. 침입자인 경우에 비밀번호를 모르고 인증을 시도할 것이다. 반면에 등록된 본인이라도 실수로 비밀번호를 잘못 입력할 경우가 있을 것이다. 따라서 비밀번호의 입력 히스토리를 저장하고, 잘못된 비밀번호의 입력 회수가 누적됨에 따라 단계적으로 생체 인식기의 문턱값을 상향 조정하게 하여 보안수준을 가변할 수 있다. 이를 위하여 구비되는 단계들을 다음과 같이 설명한다.

<53> 도 3에 도시된 S300 ~ S310 단계는, 도 2에 도시된 S200 ~ S210 단계와 같다.

<54> S312 단계에서는, 사용자가 인증되지 않은 경우에는 비밀번호 입력 히스토리를 이용하여 제1 문턱값 및 제2 문턱값을 변경하고 S300 단계로 진행한다. 여기서 S312 단계는, 잘못된 비밀번호의 입력이 n회 이상인 경우에 보안 수준을 높이도록 제1 문턱값 및 상기 제2 문턱값을 변경하는 단계를 포함할 수 있다.

<55> 또한 S312 단계는, 보안 수준을 높이도록 제1 문턱값 및 제2 문턱값이 변경된 후에, 올바른 비밀번호의 입력이 m회 이상인 경우, 보안 수준을 높이기 전의 문턱값으로 환원하는 단계를 포함할 수 있는데, 이는 다시 FRR이 낮아지도록 보안 수준을 낮게 설정하는 것이다.

<56> 비밀번호 입력 히스토리 분석을 이용하여 문턱값을 조정하는 사용자 인증 방법의 구체적인 일 실시예를 표 1을 참조하여 다음과 같이 설명한다.

<57> 연속된 인증 과정에서 잘못된 비밀번호가 3회 입력된 경우를 상정한다. 4회째에 올바르게 비밀번호를 입력하면 (FAR, FRR)=(0.20%, 15.28%)를 적용하고, 4회째에도 틀리게 비밀번호를 입력하면 (FAR, FRR)=(0.00%, 41.48%)를 적용한다. 이 때, FRR과 FAR은 다음 수학적 식 3과 같다.

<58> 【수학적 식 3】  $FRR = 1.0 \times 15.28 + 0.0 \times 42.48 = 15.28 \%$

<59>  $FAR = 0.1 \times 0.20 + 0.9 \times 0.00 = 0.02 \%$

<60> 결국 본 발명에 의한 비밀번호 입력 히스토리 분석을 이용하여 문턱값을 조정하는 사용자 인증 방법에 의하여 얻어지는 (FAR, FRR) 성능은, 이중 문턱값을 이용할 때의 (0.19%, 8.24%)에서 (0.02%, 15.28%)로 변경된다. 잘못된 비밀번호를 연속하여 3회 입력하면 보안 수준이 향상된다.

<61> 도 4는 도 1에 도시된 실시예에, 인증키를 갱신하는 단계들이 추가된 실시예를 설명하기 위한 플로우차트이다. 생체 인증키는 본인의 외모에 대한 취향이 변하는 등 시간이 자남에 따라 변할 수 있다. 이러한 경우에는, 인증키를 최신의 것으로 갱신할 필요가 있다. 또한 단말기를 사용하는 환경이 변함에 따라, 여러개의 인증키를 등록해 놓는 것이 본인에게 편리한 경우가 있다. 이러한 경우에는, 인증키를 추가할 필요가 있다. 이를 위하여 구비되는 단계들을 다음과 같이 설명한다.

<62> 도 4에 도시된 S400 ~ S408 단계는, 도 1에 도시된 S100 ~ S108 단계와 같다.

<63> S410 단계에서는, 인증키를 갱신할 것인가를 판단한다. 만일 침입자가 우연히 인증에 성공한 경우에도 인증키가 자동 갱신되면, 본 발명에 있어서의 인증키 갱신 목적과 무관하게 침입자에게 영구적인 단말기 사용을 허가하는 것이 된다. 이를 방지하기 위하



여 마련되는 S410 단계에서는, 보통의 사용자 인증보다는 엄격한 제한 조건을 가하여 인증키를 갱신할 필요가 있다.

<64> 인증키 갱신을 위한 제한 조건의 일 예로서, 입력된 비밀번호가 등록된 비밀번호와 일치하고, 생체 인식기에 의해 사용자가 인증된 경우에만 인증키를 추가/갱신하게 할 수 있다.

<65> 인증키 갱신을 위한 제한 조건을 보다 엄격히 하는 다른 예로서, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 제3 문턱치 이상으로서 사용자가 인증이 성공한 경우에만 인증키를 추가/갱신하게 할 수 있다.

<66> 인증키를 업데이트할 때, 하나의 문턱치만을 사용할 경우에 침입자가 업데이트될 가능성을 FUR(False Update Rate)이라 하면, 침입자가 비밀번호를 올바르게 입력할 확률은 10%(=0.1)이므로 FUR은 다음 수학적 식 4와 같이 구해진다. 이 때, 본인이 업데이트 되지 않을 확률은 설정된 FRR = 8.24% 그대로 이다.

<67> 【수학적 식 4】  $FUR = 0.1 \times 1.00 = 0.10 \%$

<68> 다음으로, 제3 문턱치 이상으로서 사용자 인증이 성공한 경우에만 인증키 업데이트를 허용한다면 침입자가 업데이트될 확률을 매우 줄일 수 있다. 예컨대 (FAR, FRR)=(0.01%, 26.25%)를 인증키 업데이트의 문턱치로 사용한다면, 침입자가 업데이트될 확률을 수학적 식 5와 같다.

<69> 【수학적 식 5】  $FUR = 0.1 \times 0.01 = 0.001 \%$

<70> 도 5는 도 1 내지 도 4에 도시된 실시예들이 모두 결합된 실시예를 설명하기 위한 플로우차트이다. 각 단계들은 도 1 내지 도 4에서 설명된 바와 같다.

- <71> 이하에서는 도 1 내지 도 5에 도시된 본 발명에 바람직한 실시예에 의한 사용자 인증 방법을 수행하는 사용자 인증 장치의 구성 및 동작을 설명한다.
- <72> 도 6은 본 발명에 의한 사용자 인증 장치의 바람직한 일 실시예를 설명하기 위한 블록도로서, 비밀번호 입력부(10), 문턱값 설정부(20), 저장부(30) 및 생체 인식기(40)를 포함하며, 카운터(50)를 선택적으로 더 포함한다.
- <73> 본 발명에 의한 사용자 인증 장치는, 외부로부터 입력된 하나 이상의 숫자 또는 문자에 의한 비밀번호와, 지문, 홍채, 얼굴 등의 사용자의 생체 인식 정보에 의하여 사용자를 인증한다.
- <74> 비밀번호 입력부(10)는 외부로부터 비밀번호가 입력되었는가를 판단한다. 비밀번호 입력부(10)는 사용자에 의해 조작되어 하나 이상의 숫자 또는 문자로서 입력된 비밀번호와 저장부(30)에 등록되어 있는 비밀번호를 비교하고 그 일치 여부를 출력한다.
- <75> 문턱값 설정부(20)는, 비밀번호가 입력된 경우에, 비밀번호가 등록된 비밀번호와 일치하면 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정하고, 비밀번호가 등록된 비밀번호와 일치하지 않으면 FAR을 낮춘 제2 문턱값으로 설정한다.
- <76> 저장부(30)는 등록된 비밀번호 및 등록된 생체 인식 정보를 저장하고 있다.
- <77> 생체 인식기(40)는 외부로부터 생체 인식 정보를 획득하고, 획득된 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 정합 정도를 결정하고, 정합 정도가 문턱값 이상인 경우에 사용자를 인증한다.
- <78> 도 2에 도시된 S208 단계를 수행하기 위하여, 저장부(30)는 비밀번호 입력부로부터 입력된 비밀번호의 히스토리를 저장할 수 있다. 또한, S212 단계를 수행하기 위하여 생

체 인식기(40)는, 사용자가 인증되지 않은 경우에 비밀번호 입력 히스토리를 이용하여 침입여부를 결정할 수 있다. 이 경우에, 저장부(30)는 침입이라고 결정된 경우에 입력된 침입자의 생체 인식 정보를 저장하고, 생체 인식기(40)는, 생체 인식기 입력값과 저장된 침입자의 생체 인식 정보를 비교하여 사용자가 인증되었는가를 결정하도록 구현될 수 있다.

<79> 도 3에 도시된 S308 단계를 수행하기 위하여, 저장부(30)는 비밀번호 입력부로부터 입력된 비밀번호의 히스토리를 저장할 수 있다. 또한, S312 단계를 수행하기 위하여 문턱값 설정부(20)는, 사용자가 인증되지 않은 경우에 저장된 비밀번호 입력 히스토리를 이용하여 제1 문턱값 및 제2 문턱값을 변경할 수 있다. 이 경우, 문턱값 설정부(20)는, 잘못된 비밀번호의 입력이  $n$ 회 이상인 경우에 보안 수준을 높이도록 제1 문턱값 및 제2 문턱값을 변경하도록 구현될 수 있다. 또한 문턱값 설정부(20)는, 보안 수준을 높이도록 제1 문턱값 및 제2 문턱값이 변경된 후에, 올바른 비밀번호의 입력이  $m$ 회 이상인 경우에, 보안 수준을 높이기 전의 문턱값으로 환원하도록 구현될 수 있다.

<80> 본 발명에 의한 사용자 인증 장치는, 도 4에 도시된 S410 단계 및 S412 단계를 수행하기 위하여, 사용자가 인증된 경우에 인증키를 추가/갱신할 수 있다. 인증키를 추가/갱신하기 위하여, 생체 인식기(40)는 인증이 성공한 경우에, 획득된 생체 인식 정보를 저장부(30)로 출력한다. 특히, 생체 인식기(40)는, 인증키 갱신의 신뢰성을 높이기 위하여, 비밀번호 입력부(10)에 의해 입력된 비밀번호가 등록된 비밀번호와 일치하고, 생체 인식기(40)에 의해 사용자가 인증된 경우에만, 획득된 생체 인식 정보를 저장부(30)로 출력하여, 인증키를 추가/갱신하도록 구현될 수 있다. 또한 본 발명에 의한 사용자 인증

장치는, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 제3 문턱치 이상인 경우에만 인증키를 추가/갱신하도록 구현될 수도 있다.

<81> 카운터(50)는 S212 단계 및 S312 단계를 수행하기 위하여, 선택적으로 더 구비된다. 카운터(50)는 비밀번호가 잘못 입력된 회수를 카운트하여 카운트 결과로서 출력한다. 이 때 문턱값 설정부(20)는 카운트 결과에 따라 문턱값을 단계적으로 조정할 수도 있다. 또한 생체 인식기(40)는 카운트 결과에 따라 침입 여부를 결정하고, 침입이라고 결정되면 획득된 생체 인식 정보를 저장부(30)로 출력하고, 저장부(30)는 생체 인식기(40)로부터 입력된 사용자의 생체 인식 정보를 저장하도록 구현될 수 있다.

<82> 한편, 전술한 본 발명의 바람직한 실시예에 의한 사용자 인증 방법(도 1 내지 도 5)은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 상기 컴퓨터로 읽을 수 있는 기록매체는 예컨대 롬, 플로피 디스크, 하드디스크 등과 같은 마그네틱 저장매체, 예컨대 씨디롬, 디브이디 등과 같은 광학적 판독매체, 및 예컨대 인터넷을 통한 전송과 같은 캐리어 웨이브와 같은 저장매체를 포함한다.

#### 【발명의 효과】

<83> 이상에서 설명한 바와 같이, 본 발명에 의한 사용자 인증 방법에 의하면, 비밀번호와 생체 인식기가 유기적으로 결합하여, 비밀번호의 입력 결과가 생체 인식기 성능에 영향을 주거나, 생체 인식 결과가 피드백되어 다음의 인증과정에 영향을 주도록 하여 FAR(False Acceptance Rate)와 FRR(False Rejection Rate)를 함께 향상시키는 효과가 있다.

<84>      본 발명은 이상에서 설명되고 도면들에 표현된 예시들에 한정되는 것은 아니다. 전술한 실시 예들에 의해 가르침 받은 당업자라면, 다음의 특허 청구 범위에 기재된 본 발명의 범위 및 목적 내에서 치환, 소거, 병합, 및 단계들의 재배치 등에 의하여 전술한 실시 예들에 대해 많은 변형이 가능할 것이다.

**【특허청구범위】****【청구항 1】**

외부로부터 입력된 하나 이상의 숫자 또는 문자에 의한 비밀번호와, 지문, 홍채, 얼굴 등의 사용자의 생체 인식 정보에 의하여 사용자를 인증하는 방법에 있어서,

(a) 비밀번호가 입력되었는가를 판단하는 단계;

(b) 비밀번호가 입력된 경우에, 상기 비밀번호가 등록된 비밀번호와 일치하면 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정하고, 상기 비밀번호가 등록된 비밀번호와 일치하지 않으면 FAR을 낮춘 제2 문턱값으로 설정하는 단계; 및

(c) 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 상기 (a) 단계로 진행하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

**【청구항 2】**

제1항에 있어서,

(d) 상기 (b) 단계 후에, 비밀번호 입력 히스토리를 저장하는 단계; 및

(e) 상기 (c) 단계 후에, 사용자가 인증되지 않은 경우에는 상기 비밀번호 입력 히스토리를 이용하여 침입여부를 판단하여, 침입이 아니라고 판단되면 상기 (a) 단계로 진행하는 단계;를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

**【청구항 3】**

제2항에 있어서,

(f) 상기 (e) 단계의 판단 결과 침입이라고 판단되면, 입력된 침입자의 생체 인식 정보를 저장하는 단계를 더 포함하고,

상기 (c) 단계는 생체 인식기 입력값과 상기 저장된 침입자의 생체 인식 정보를 비교하여 인증하는 단계를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

#### 【청구항 4】

제1항에 있어서,

(d) 상기 (b) 단계 후에, 비밀번호 입력 히스토리를 저장하는 단계; 및

(g) 상기 (c) 단계 후에, 사용자가 인증되지 않은 경우에는 상기 비밀번호 입력 히스토리를 이용하여 상기 제1 문턱값 및 상기 제2 문턱값을 변경하고 상기 (a) 단계로 진행하는 단계를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

#### 【청구항 5】

제4항에 있어서, 상기 (g) 단계는,

잘못된 비밀번호의 입력이  $n$ 회 이상인 경우에 보안 수준을 높이도록 상기 제1 문턱값 및 상기 제2 문턱값을 변경하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

#### 【청구항 6】

제5항에 있어서, 상기 (g) 단계는,

보안 수준을 높이도록 상기 제1 문턱값 및 상기 제2 문턱값이 변경된 후에, 올바른 비밀번호의 입력이  $m$ 회 이상인 경우, 상기 보안 수준을 높이기 전의 문턱값으로 환원하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

**【청구항 7】**

제1항에 있어서,

(h) 상기 (c) 단계에서 상기 생체 인식기에 의해 사용자가 인증된 경우에, 인증키를 추가/갱신하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

**【청구항 8】**

제5항에 있어서, 상기 (h) 단계는,

상기 입력된 비밀번호가 등록된 비밀번호와 일치하고, 상기 생체 인식기에 의해 사용자가 인증된 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 방법.

**【청구항 9】**

제7항 또는 제8항에 있어서, 상기 (h) 단계는,

상기 생체 인식기에 의해 사용자가 인증된 경우, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 제3 문턱치 이상인 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 방법.

**【청구항 10】**

외부로부터 입력된 하나 이상의 숫자 또는 문자에 의한 비밀번호와, 지문, 홍채, 얼굴 등의 사용자의 생체 인식 정보에 의하여 사용자를 인증하는 장치에 있어서,

외부로부터 비밀번호가 입력되었는가를 판단하는 비밀번호 입력부;

등록된 비밀번호 및 등록된 생체 인식 정보를 저장하는 저장부;

비밀번호가 입력된 경우에, 상기 비밀번호가 상기 등록된 비밀번호와 일치하면 생체 인식기에서 사용되는 문턱값을 FRR을 낮춘 제1 문턱값으로 설정하고, 상기 비밀번호



가 상기 등록된 비밀번호와 일치하지 않으면 FAR을 낮춘 제2 문턱값으로 설정하는 문턱값 설정부; 및

외부로부터 생체 인식 정보를 획득하고, 상기 획득된 생체 인식 정보와 상기 등록된 생체 인식 정보를 비교하여 정합 정도를 결정하고, 상기 정합 정도가 상기 문턱값 이상인 경우에 사용자를 인증하는 생체 인식기를 포함하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 11】

제10항에 있어서,

상기 저장부는 상기 비밀번호 입력부로부터 입력된 비밀번호의 히스토리를 저장하고,

상기 생체 인식기는, 사용자가 인증되지 않은 경우에 상기 비밀번호 입력 히스토리를 이용하여 침입여부를 결정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 12】

제11항에 있어서,

상기 저장부는 침입이라고 결정된 경우에 입력된 침입자의 생체 인식 정보를 저장하고,

상기 생체 인식기는, 생체 인식기 입력값과 상기 저장된 침입자의 생체 인식 정보를 비교하여 사용자가 인증되었는가를 결정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 13】

제10항에 있어서,

상기 저장부는 상기 비밀번호 입력부로부터 입력된 비밀번호의 히스토리를 저장하고,

상기 문턱값 설정부는, 사용자가 인증되지 않은 경우에 상기 저장된 비밀번호 입력 히스토리를 이용하여 상기 제1 문턱값 및 상기 제2 문턱값을 변경하는 것을 특징으로 하는 사용자 인증 장치.

**【청구항 14】**

제13항에 있어서, 상기 문턱값 설정부는,

잘못된 비밀번호의 입력이  $n$ 회 이상인 경우에 보안 수준을 높이도록 상기 제1 문턱값 및 상기 제2 문턱값을 변경하는 것을 특징으로 하는 사용자 인증 장치.

**【청구항 15】**

제14항에 있어서, 상기 문턱값 설정부는,

보안 수준을 높이도록 상기 제1 문턱값 및 상기 제2 문턱값이 변경된 후에, 올바른 비밀번호의 입력이  $m$ 회 이상인 경우에, 상기 보안 수준을 높이기 전의 문턱값으로 환원하는 것을 특징으로 하는 사용자 인증 장치.

**【청구항 16】**

제10항에 있어서,

사용자가 인증된 경우에 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 장치.

**【청구항 17】**

제16항에 있어서,

상기 비밀번호 입력부에 의해 입력된 비밀번호가 등록된 비밀번호와 일치하고, 상기 생체 인식기에 의해 사용자가 인증된 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 18】

제16항 또는 제17항에 있어서,

입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 제3 문턱치 이상인 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 19】

제10항에 있어서, 상기 사용자 인증 장치는,

잘못된 비밀번호 입력 회수를 카운트하여 카운트 결과를 출력하는 카운터를 더 포함하며,

상기 문턱값 설정부는 상기 카운트 결과에 따라 문턱값을 가변하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 20】

제19항에 있어서, 상기 사용자 인증 장치는,

잘못된 비밀번호 입력 회수를 카운트하여 카운트 결과를 출력하는 카운터를 더 포함하며,

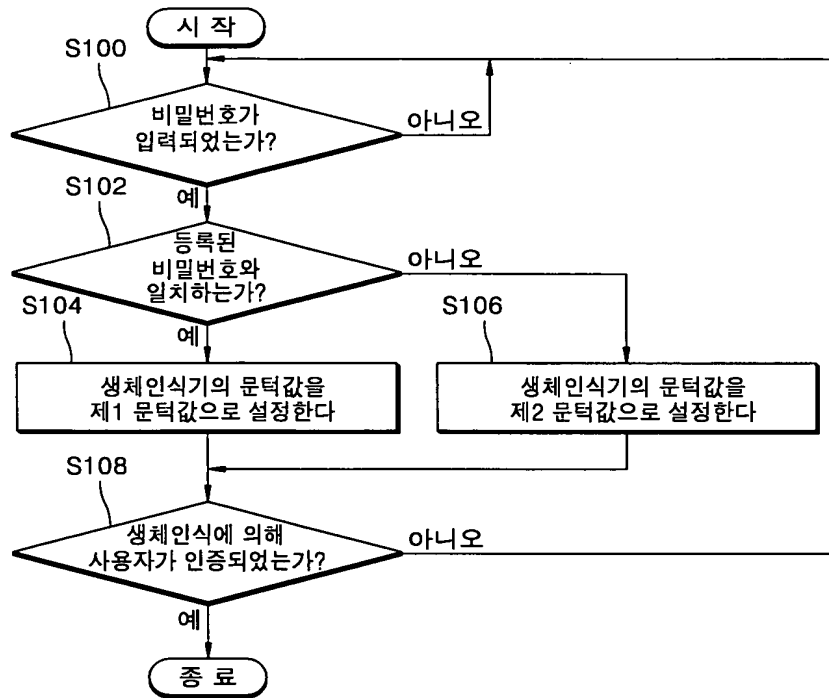
상기 저장부는 상기 카운트 결과에 따라 상기 생체 인식기로부터 획득된 사용자의 생체 인식 정보를 저장하는 것을 특징으로 하는 사용자 인증 장치..

【청구항 21】

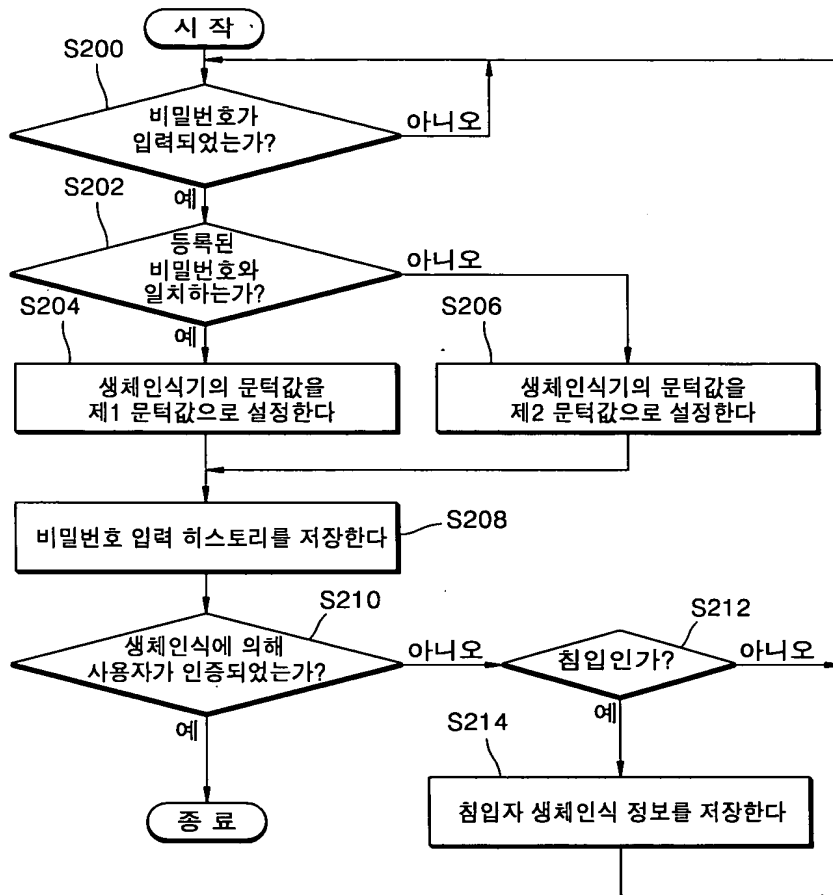
제1 항 내지 제9 항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

## 【도면】

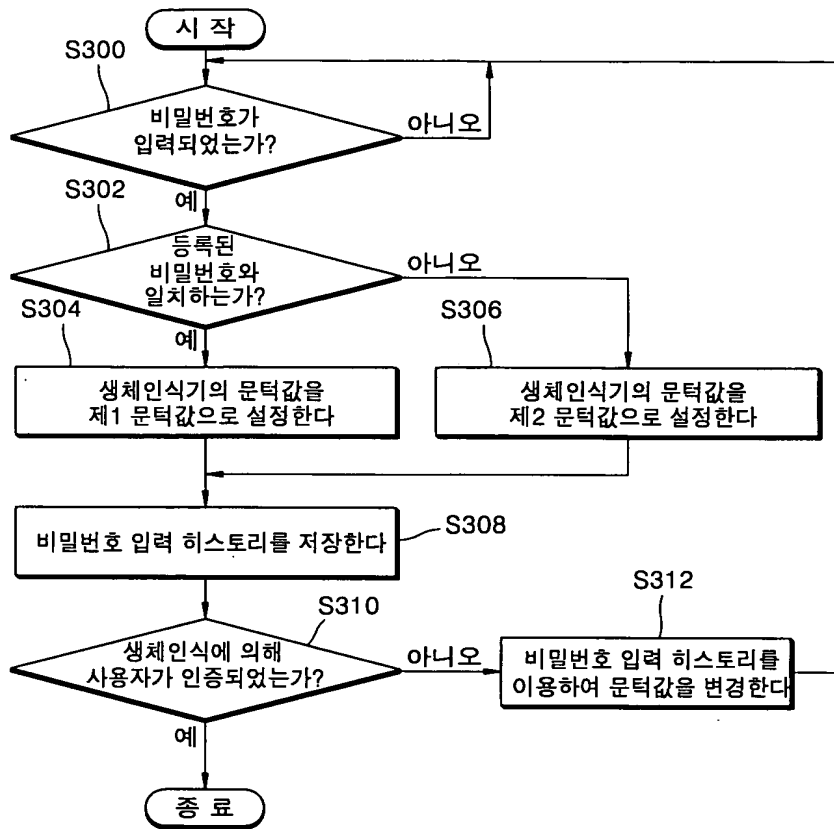
【도 1】



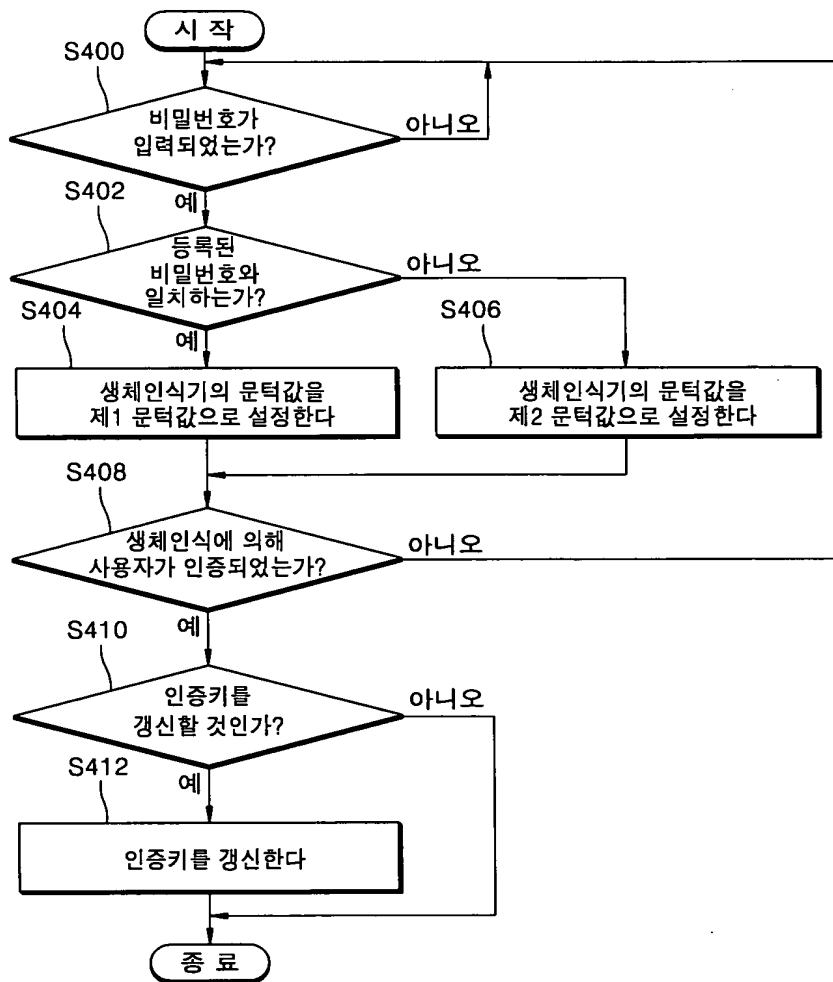
【도 2】



【도 3】

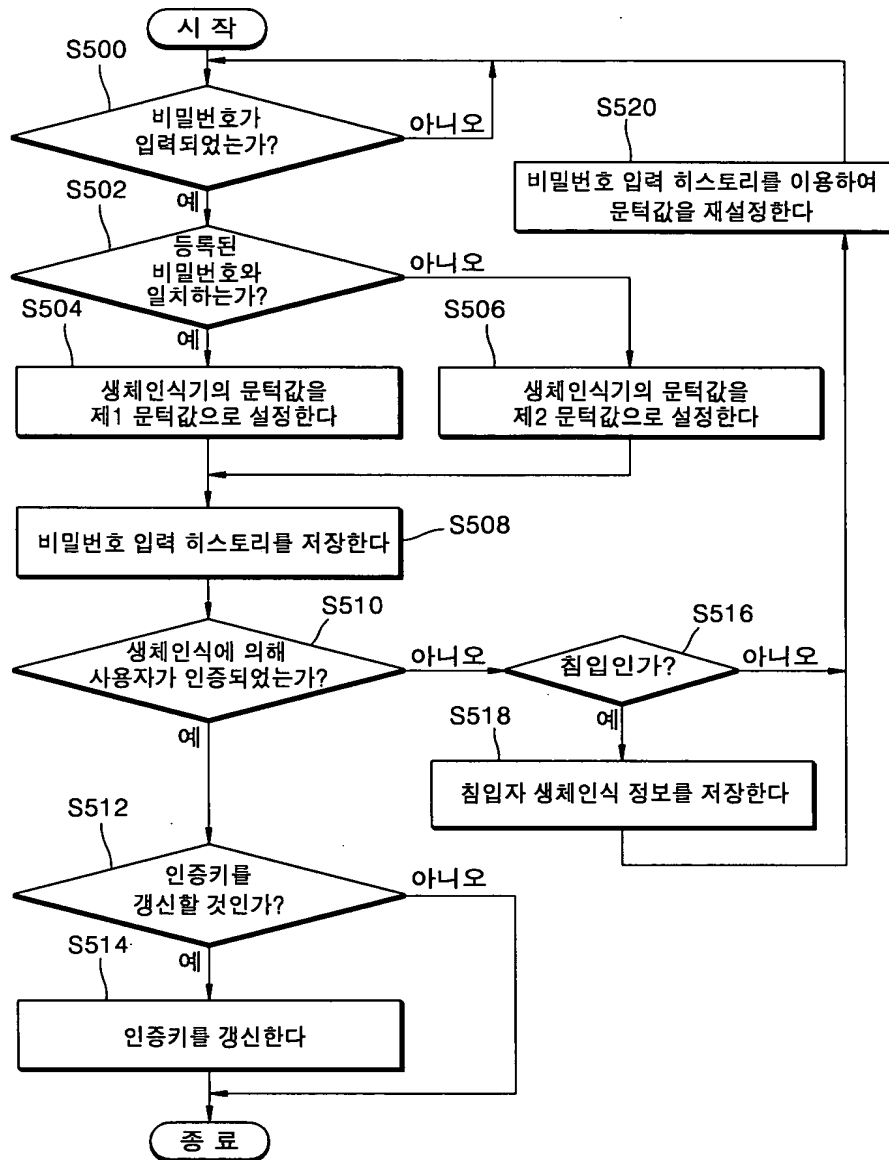


【도 4】





【도 5】



【도 6】

